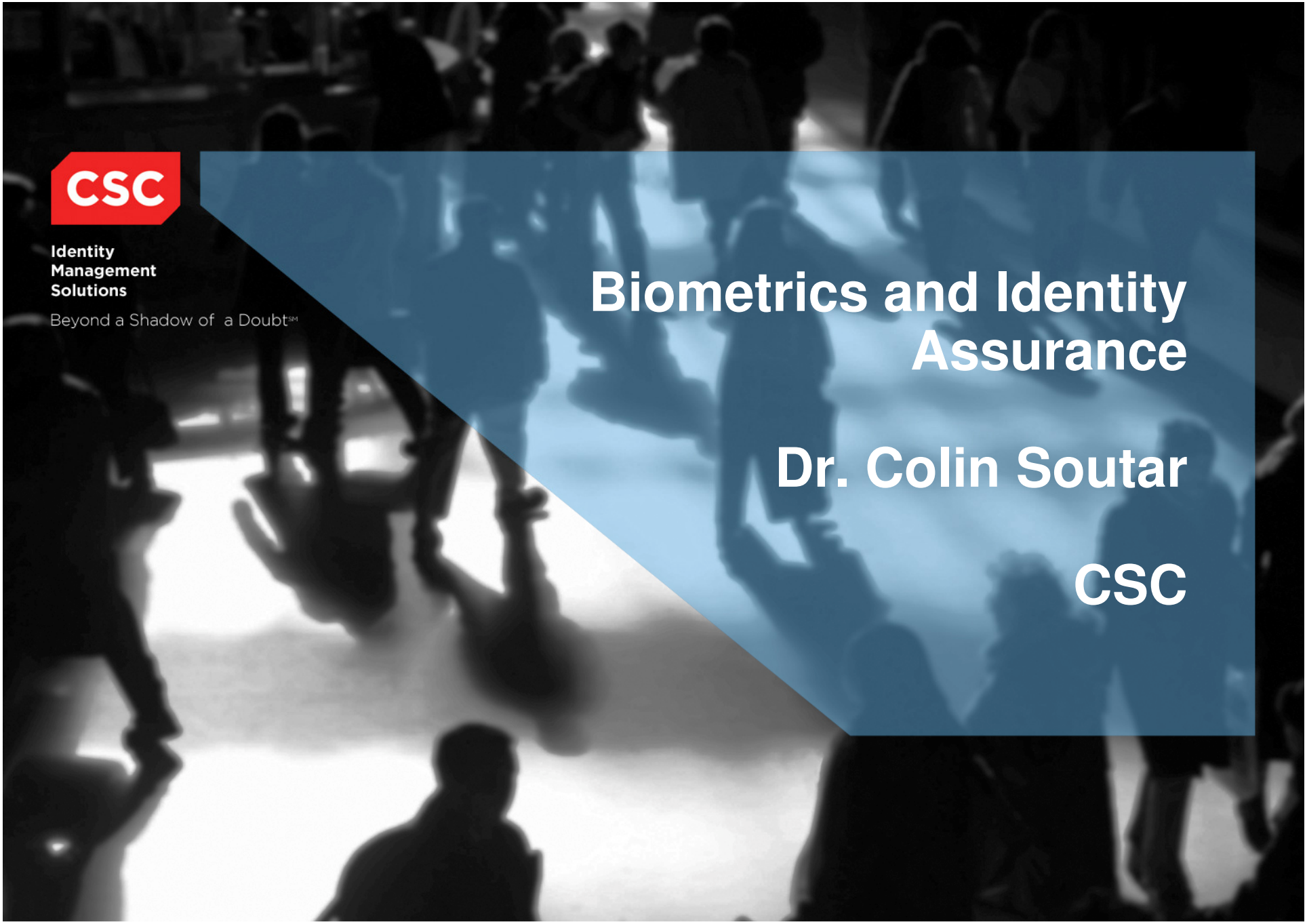


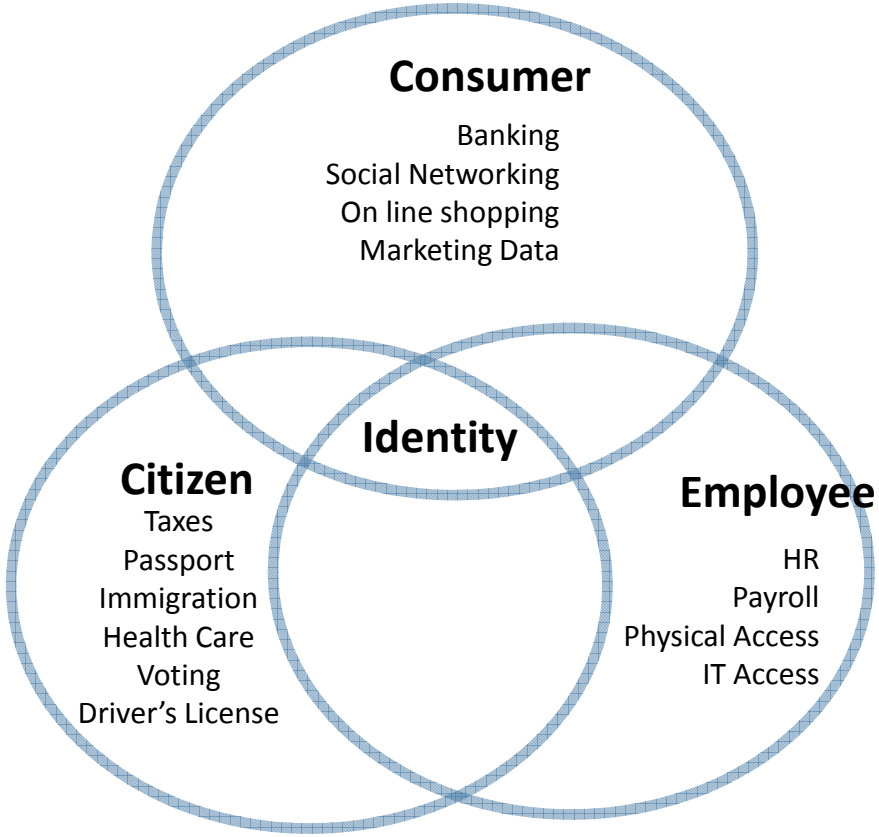
Biometrics and Identity Assurance

Dr. Colin Soutar

CSC

Identity

- Identity is no longer solely based on physical credentials
- Identity is becoming an entity that is independent from entitlements
- Access to identity-enabled applications is becoming more ubiquitous (internet, cell-phones etc.)



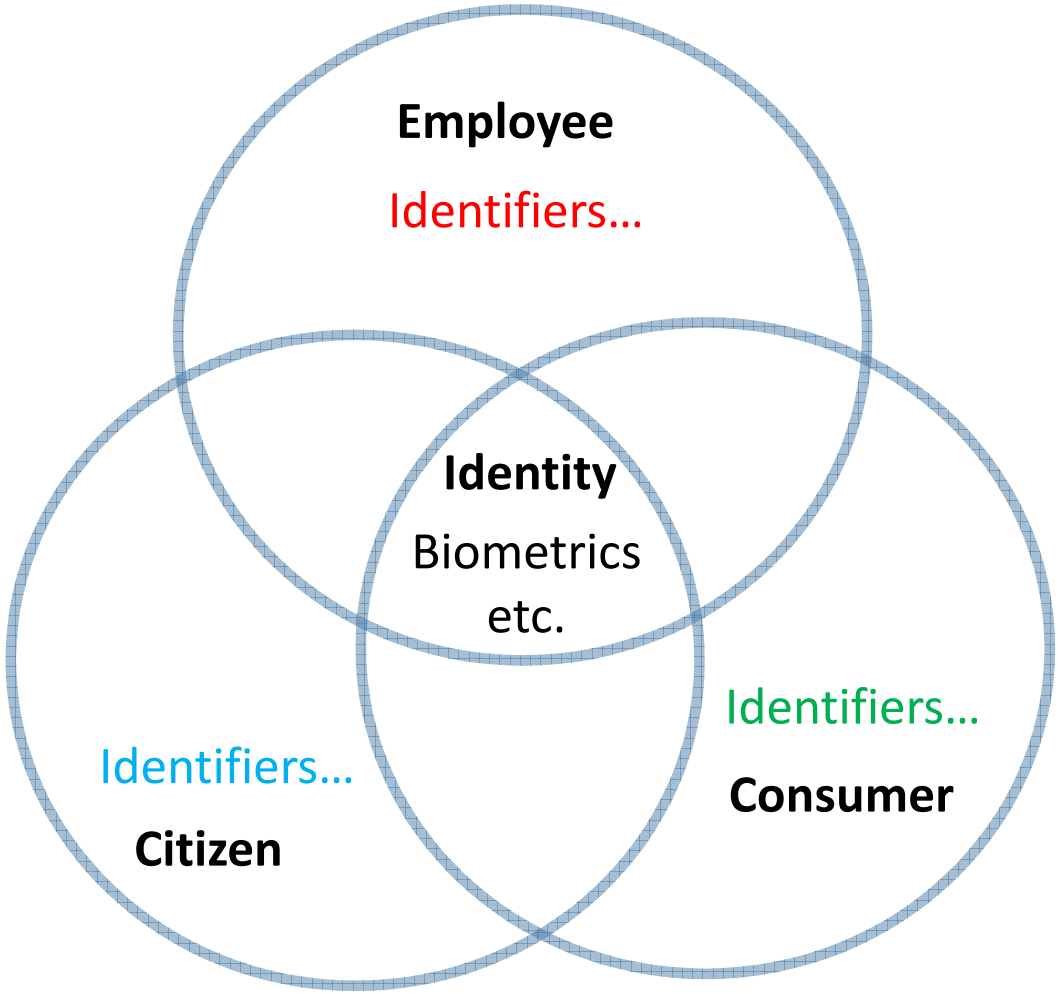
Identity and Biometrics

- ***Identity*** **of an** ***Individual*** **is established as a composite of various components of Personally Identifiable Information (PII):**
  - **Biographical information – name, DOB, address, etc.**
  - **Physiological information – i.e. biometrics**
  - **Documents – passports, birth certificate**
  - **Events and knowledge – i.e. high school, memorable place, mother's maiden name**
- **Identity Proofing**
  - **Determination of the uniqueness of an Individual's claimed Identity**
- **Identity Management System**
  - **Governs the permissions, privileges, benefits and rights (*Entitlements*) of an individual within an *Enterprise***
  - **The requirements for establishing an "Enterprise Identity" are usually a subset of Identity**
  - **A *Credential* that links the Enterprise Entitlement to the Individual is usually issued (a physical or logical token)**
  - **Identity Authentication is used to verify that the individual is the valid "holder" of the credential**
  - **Authorization is an Enterprise-level function that verifies that the individual is currently eligible for the entitlement**

Privacy

- Jurisdictionally-defined rights and obligations
- Individual Control of Personal and Identity Information
- Biometric data is Personally Identifiable Information (PII) AND Identity Data
- Consent, Limited Use, Safeguards, Data Protection

Identity/Identifiers/Authorization

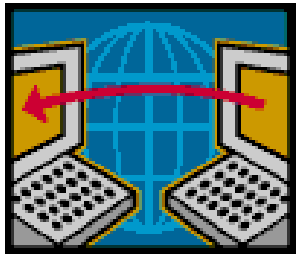


Identity and Privacy Assurance

Individual

Safeguarding of Identity Data

Levels of Identity Assurance



Privacy Assurance

Identity Assurance

Identity Assurance -> Enterprise

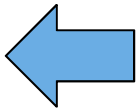
Identity Assurance (transaction)	=	Identity Authentication (transaction)	+	Identity Proofing (enrollment)
Ability to Support Level of Assurance (LOA)		Strength of Performance Assurance of Conformance		Uniqueness of Identity Interoperability

Biometric Identification and Verification

- Biometric Identification used as part of Identity Proofing
- Biometrics for Identity Proofing needs to be able to distinguish individuals in a large population
- Biometric Verification used on a daily basis as part of an authentication mechanism
- Biometric Verification modality or algorithms (and thus templates) need not be the same.
- Verification needs to authenticate a user to a certain assurance level

Privacy Assurance -> Individual

Identity Assurance (transaction)



Identity Authentication (transaction)

+

Identity Proofing (enrollment)

Enables transaction and protects Account

Maintains ongoing Integrity of Identity Data

Establishes Uniqueness for Entitlement Rights

Kantara Identity Assurance Framework

- Establish the trustworthiness of Services in Identity system
- c.f. the delegation of trust via PKI or other architecture

- Common Operating Criteria (CO)
- Credential Management (CM)
- ID Proofing (ID)

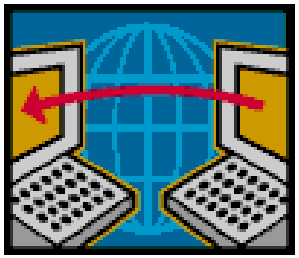
- Privacy Profile

- Some privacy environments require separation of CM and ID

Identity Assurance

Levels of Identity Assurance

Risk



- **To:**
  - **Enterprise**
    - **Entitlement Fraud**
    - **Security Breach**
  - **Individual**
    - **Privacy Breach**
    - **Loss of Privilege**

Risk – Biometric Technologies

- False Results, Security Breach, Spoofing

- Relatively Mature and Controllable in Identity Proofing Scenarios
  - Large scale system evaluation
  - Supervised
    - Mitigates spoofing
  - Secure Storage

- Not so well defined in Identity Authentication Scenarios
  - Remote authentication
  - Non-supervised
  - Varying Systems (and Performance)
    - Sensors
    - Algorithms
  - Conformance required, not necessarily interoperability

INCITS M1 Ad Hoc on E-authentication (2005)

- There is a role for biometric authentication at each of the four assurance levels defined in OMB M-04-04
  - Map Levels of Performance to resulting level of Identity Assurance
- Biometric authentication can provide significant benefits in certain situations, not least of which is the tight binding of the authentication event to the physical presence of a human claimant
  - Evaluate Biometric Performance on Varied Platforms
- Some additional challenges and threats accompany the use of biometric authentication, but countermeasures exist to address them
  - Vulnerability Testing
- Biometrics present a different paradigm than traditional authentication methods where authentication data is always secret.
  - Evaluate Template Protection Techniques
  - Align quantified performance with other authentication factors

Conclusions

- Mobile devices are being used to access more applications
  - Need to bind device to individual
  - Many mobile devices available with biometric technologies
  - Lack of clarity on Identity and Privacy Assurance capabilities
- Biometrics can be used to strongly bind an individual to identity.
  - Mitigate Identity Theft and protect personal data
  - Provide a strong degree of Identity Assurance
  - Trusted Identities as the basis for Identity Federation
- Identity and Privacy Assurance relies on two distinct processes:
  - Identity Proofing and Identity Authentication
  - Potentially different Privacy, Interoperability and Performance Requirements
- Biometrics need to demonstrate system conformance and quantifiable performance.
  - ISO SC27 WG5, ISO SC37 WG 6, ITU-T SG17, and others on IDM and privacy
  - Common Criteria
  - NVLAP 150-25


CSC
Identity
Management
Solutions
Beyond a Shadow of a Doubt℠
Questions?
csoutar@csc.com
416 644 8640.